



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

AF
JFW

Applicant: Sean Brennan

Title: SYSTEM AND METHOD FOR ACCOMPLISHING TWO-FACTOR USER
AUTHENTICATION USING THE INTERNET

Docket No.: 105.215US1

Serial No.: 10/050,752

Filed: January 16, 2002

Due Date: October 14, 2006 (Saturday)

Examiner: Michael J. Simitoski

Group Art Unit: 2134

MS Appeal Brief - Patents

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

We are transmitting herewith the following attached items (as indicated with an "X"):

☒ Return postcard.

☒ Appeal Brief under 37 CFR 41.37 (27 pgs.).

☒ Permission to charge Deposit Account No. 19-0743 in the amount of \$250.00 to cover the Appeal Brief Filing fee.

Please consider this a PETITION FOR EXTENSION OF TIME for sufficient number of months to enter these papers and please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.

Customer Number 21186

By: Thomas F. Brennan
Atty: Thomas F. Brennan
Reg. No. 35,075

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: MS Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 16th day of October, 2006.

Name

Amy Moriarty

Signature

[Signature]

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.

(GENERAL)



APPEAL BRIEF UNDER 37 C.F.R. § 41.37

TABLE OF CONTENTS

	<u>Page</u>
<u>1. REAL PARTY IN INTEREST</u>	2
<u>2. RELATED APPEALS AND INTERFERENCES</u>	3
<u>3. STATUS OF THE CLAIMS</u>	4
<u>4. STATUS OF AMENDMENTS</u>	5
<u>5. SUMMARY OF CLAIMED SUBJECT MATTER</u>	6
<u>6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL</u>	9
<u>7. ARGUMENT</u>	10
<u>8. SUMMARY</u>	19
<u>CLAIMS APPENDIX</u>	21
<u>EXHIBIT APPENDIX</u>	25
<u>RELATED PROCEEDINGS APPENDIX</u>	26



PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Sean Brennan

Examiner: Michael J. Simitoski

Serial No.: 10/050,752

Group Art Unit: 2134

Filed: January 16, 2002

Docket: 105.215US1

For: SYSTEM AND METHOD FOR ACCOMPLISHING TWO-FACTOR USER
AUTHENTICATION USING THE INTERNET

APPEAL BRIEF UNDER 37 CFR § 41.37

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The Appeal Brief is presented in support of the Notice of Appeal to the Board of Patent Appeals and Interferences, filed on August 14, 2006, from the Final Rejection of claims 4-5, 7-13, and 16-34 of the above-identified application, as set forth in the Final Office Action mailed on April 21, 2006.

The Commissioner of Patents and Trademarks is hereby authorized to charge Deposit Account No. 19-0743 in the amount of \$250.00 which represents the requisite fee set forth in 37 C.F.R. § 41.20(b)(2). Appellant respectfully requests consideration and reversal of the Examiner's rejections of pending claims.

10/18/2006 HDEMESS1 00000102 190743 10050752

01 FC:2402 250.00 DA

1. REAL PARTY IN INTEREST

The real party in interest of the above-captioned patent application is the assignee,
SECURE COMPUTING CORPORATION.

2. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellant that will have a bearing on the Board's decision in the present appeal.

3. STATUS OF THE CLAIMS

In accordance with 37 CFR § 41.37(c)(1)(iii) requiring a statement of the status of all claims, pending and cancelled, Appellant submits the following:

The present application was filed on January 16, 2002 with claims 1-20. Claims 1-3, 14 and 15 were withdrawn from consideration under a Restriction Requirement. Claim 6 was canceled and claims 21-34 were added.

A Non-Final Office Action was mailed September 8, 2005. A Final Office Action (hereinafter “the Final Office Action”) was mailed April 14, 2006. Claims 4, 5, 7-13 and 16-20 stand twice rejected. Claims 21-34 stand once rejected.

An “Amendment Under 37 CFR §41.33(b)” was filed October 13, 2006 (before the filing of this Appeal Brief). In the Amendment, Appellant canceled claims 24-27 and 31-34.

Thus, claims 4, 5, 7-13, 16-23 and 28-30 remain pending and are subject of the present Appeal.

4. STATUS OF AMENDMENTS

The following is a statement of the status of any Amendments filed subsequent to final rejection (as required by 37 CFR §41.37(c)(1)(iv)):

An “Amendment and Response Under 37 CFR §1.116” was filed on July 14, 2006 subsequent to the Final Office Action mailed April 14, 2006. In the Amendment, claims 17, 21, 25-28 and 30-33 were amended, and claims 24 and 34 were canceled. The Amendment, however, was not entered by the Examiner as noted in the Advisory Action mailed August 3, 2006.

An “Amendment Under 37 CFR §41.33(b)” was filed October 13, 2006 (before the filing of this Appeal Brief). In the Amendment, Appellant canceled claims 24-27 and 31-34.

5. SUMMARY OF CLAIMED SUBJECT MATTER

This summary is presented in compliance with the requirements of Title 37 C.F.R. § 41.37(c)(1)(v), mandating a “concise explanation of the subject matter defined in each of the independent claims involved in the appeal ...”

Nothing contained in this summary is intended to change the specific language of the claims described, nor is the language of this summary to be construed so as to limit the scope of the claims in any way. Each claim involved in the present appeal is supported by the specification and/or drawings.

As noted in the Background of the present patent application, access to computer network, web site and the like is more and more controlled by some type of security procedures, creating a need for improved security method and system. Conventional security procedures require user names and passwords for allowing access to sensitive information at web site. Although this provides a level of security, it can be breached by several relatively easy means, such as observance of a user or interception of the login signal as they are transmitted over the network or internet.

As described by Applicant at p. 9, lines 2-3 and shown in Fig. 1, Applicant describes and claims a system and method for accomplishing two-factor authentication using the internet. The method taught by Appellant and claimed in claims 4, 5, 7-13, 16-20 employs using two separate user authentication methods at two web sites over the internet (p. 4, lines 8-9; Fig. 1).

As described by Appellant at p. 9, lines 3-18 and claimed in claim 4, Appellant’s two-factor authentication method and system comprises providing two user authentication methods selected to authenticate two factors associated with the user (e.g., a password and a token code), enabling a user to communicate authentication data for both authentication methods to a first web site, authenticating the user at the first web site using the first authentication method, enabling the communication of at least some of the authentication data from the first web site to a second web site and authenticating the user at the second web site based on the authentication data transferred from the first web site using the second authentication method. In this way, both the login site and the security site are involved in user authentication using at least one factor of a different type, respectively. This also allows the login site to determine restrictive access by the

user to the required data such as admitting or denying an entry to the user based on the results of the two authentications (p. 4, lines 4-6; p. 6, lines 15-16).

For example, in one approach, a user is required, upon login to a secure web site, to enter at least a code generated by the user's token for later use in a security site (p. 6, lines 12-15). The user may be further required to enter a user name and user password to the login web site (p. 6, lines 17). Once the authentication data for both sites are entered, the login site authenticates the user using the user name and user password (p. 6, lines 18-19). When the authentication at the login site is done, the user's token code is passed from the login site to the security site (p. 6, lines 13-14; p. 7, lines 11-12). Then, the security site authenticates the user's identity by verifying whether or not the user's token code was generated by the user's token (p. 6, lines 14-15). The verification result from the security site is passed back to the login site (p. 4, line 5).

Appellant teaches, and claims in claims 5, 7 and 8, the first web site initially authenticating the user based on the data relating to the first authentication method (p. 4, lines 16-17; p. 7, lines 14-16).

Appellant teaches, and claims in claims 7 and 8, the first web site communicating with the second web site only if the user is initially authenticated (p. 4, lines 18-19; p. 7, lines 17-19).

Appellant teaches, and claims in claim 8, the first web site communicating to the second web site at least data relating to the second authentication method, and user identification data (p. 4, lines 19-21; p. 7, lines 19-20).

Appellant teaches, and claims in claims 10-13 and 20, one authentication method employing a token (p. 4, line 22 through p. 5, line 5).

Appellant teaches, and claims in claims 16-17, one authentication method employing a fixed complex code (p. 8, lines 4-7).

Appellant teaches, and claims in claims 21-23, a method of authenticating a user to one or more web sites. As shown at p. 8, line 6, p. 9, lines 2-16, and Fig. 1, the method comprises authenticating the user to a first web site of the one or more web sites and authenticating the user to a second web site once authenticated to the first web site. The method grants the user access to content on the first web site only if he is authenticated to both the first and second web sites (p. 4, line 4-6; p. 6, lines 15-16; p. 9, lines 16-18).

Appellant teaches, and claims in claims 22, authenticating to the first web site using a password and authenticating to the second web site using a token (p. 3, lines 20 through p. 4, line 6; p. 4, lines 16-23; p. 7, lines 14-22).

Appellant teaches, and claims in claim 23, authenticating to the first web site using a password and authenticating to the second web site using a one-time password (p. 4, line 22 through p. 5, line 10).

Appellant teaches, and claims in claims 28-30, an authentication system. As shown at p. 3, line 20 through p. 4, line 21, p. 8, line 6, p. 9, lines 2-18 and Fig. 1, 4 & 5, the system comprises one or more web sites implementing a first authentication method and an authentication web site connected to the one or more web sites for implementing a second authentication method. The system receives authentication information for the second authentication method via a first web site of the one or more web sites and transfers it to the authentication web site. The system grants a user access to content on the one or more web sites only if authenticated to both the first web site and the authentication web site (p. 4, line 4-6; p. 6, lines 15-16; p. 9, lines 16-18).

Appellant teaches, and claims in claims 29, the first authentication method based on a password and the second authentication method based on a token (p. 3, lines 20 through p. 4, line 6; p. 4, lines 16-23; p. 7, lines 14-22).

Appellant teaches, and claims in claim 30, the first authentication method based on a password and the second authentication method based on a one-time password (p. 4, line 22 through p. 5, line 10).

This summary does not provide an exhaustive or exclusive view of the present subject matter, and Appellant refers to the appended claims and their legal equivalents for a complete statement of the inventive subject matter.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 4, 5, 7-9, 18, 21 and 28 are rejected under 35 USC § 103(a) as being unpatentable over Ying et al. (U.S. Patent 6,853,980, hereinafter ‘Ying’) and Krueger et al. (U.S. Patent Application Publication 2002/0077837, hereinafter ‘Krueger’).

Claims 10-12, 19-20, 22-23 and 29-30 are rejected under 35 USC § 103(a) as being unpatentable over Ying and Krueger, as applied to claims 21 and 28 above, in further view of “RSA Web-Security Portfolio; How RSA SecureID Agents Can Secure Your Website” (hereinafter ‘RSA’).

Claim 13 is rejected under 35 USC § 103(a) as being unpatentable over Ying, Krueger and RSA, as applied to claim 11 above, in further view of Tan et al. (U.S. Patent Application Publication 2001/0045451, hereinafter ‘Tan’) and “eToken: The Key to Security for the Internet Age” (hereinafter ‘Aladdin’).

Claim 16 and 17 are rejected under 35 USC § 103(a) as being unpatentable over Ying, Krueger and RSA, as applied to claim 4 above, in further view of “Network Security Essentials Applications and Standards” (hereinafter ‘Stallings’).

7. ARGUMENT

Rejections under U.S.C. § 103

1) The Applicable Law

According to *M.P.E.P.* § 2141, which cites *Hodosh v. Block Drug Co., Inc.*, 786 F.2d 1136, 1143 n.5, 229 USPQ 182, 187 n.5 (Fed. Cir. 1986), the following tenets of patent law must be adhered to when applying 35 U.S.C. § 103. First, the claimed invention must be considered as a whole. Second, the references must be considered as a whole and must suggest the desirability and thus the obviousness of making the combination. Third, the references must be viewed without the benefit of impermissible hindsight vision afforded by the claimed invention. Fourth, obviousness is determined using a reasonable expectation of success standard. Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. *M.P.E.P.* § 2141 (citing *Graham v. John Deere*, 383 U.S. 1, 148 USPQ 459 (1966)).

The Examiner has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *M.P.E.P.* § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)).

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on Appellants' disclosure. *M.P.E.P.* § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). The references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references. *M.P.E.P.* § 2142 (citing *Ex parte Clapp*, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985)). In considering the disclosure of a reference, it is proper to take into account not only specific teachings of the

reference but also the inferences which one skilled in the art would reasonably be expected to draw there from. *M.P.E.P.* § 2144.01 (citing *In re Preda*, 401 F.2d 825, 826, 159 USPQ 342, 344 (CCPA 1968)). However, if the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *M.P.E.P.* § 2143.01 (citing *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984)).

In order to take into account the inferences which one skilled in the art would reasonably make, the examiner must ascertain what would have been obvious to one of ordinary skill in the art at the time the invention was made. *M.P.E.P.* § 2141.03 (citing *Environmental Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 218 USPQ 865 (Fed. Cir. 1983), *cert. denied*, 464 U.S. 1043 (1984)).

The examiner must step backward in time and into the shoes worn by the hypothetical “person of ordinary skill in the art” when the invention was unknown and just before it was made. In view of all factual information, the examiner must then make a determination whether the claimed invention “as a whole” would have been obvious at that time to that person. Knowledge of Appellants’ disclosure must be put aside in reaching this determination, yet kept in mind in order to determine the “differences,” conduct the search and evaluate the “subject matter as a whole” of the invention. The tendency to resort to “hindsight” based upon Appellants’ disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art.

M.P.E.P. § 2141.03.

2) *Application of § 103 to the Rejected Claims*

Claims 4, 5, 7-9, 18, 21 and 28 were rejected under 35 USC § 103(a)

Claims 4, 5, 7-9, 18, 21 and 28 are rejected under 35 USC § 103(a) as being unpatentable over Ying et al. (U.S. Patent 6,853,980, hereinafter ‘Ying’) and Krueger et al. (U.S. Patent Application Publication 2002/0077837, hereinafter ‘Krueger’). Appellant respectfully submits that the Examiner has failed to meet his burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness.

As noted above, in order to establish a *prima facie* case of obviousness, the Examiner must meet three basic criteria. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

Neither Ying nor Krueger, however, alone or in combination, teach or suggest an authentication method and system using at least two different factors at two or more web sites as taught by Appellant and claimed in claims 4, 5, 7-9 and 18.

Applicant teaches at p. 9, lines 2-18 and claims in claims 4, 5, 7-9 and 18, a system and method for authenticating a user at two sites using at least two factors. As noted at p. 9, lines 10-18, Applicant teaches:

One of the authentication methods is accomplished at the first web site 14. Typically, this comprises verification based on the user name and password. The first web site 14 then communicates at least some of the authentication data to the second web site 16, also using the internet 12. For the preferred embodiment, the first web site 14 would transmit to the second web site 16 the token code and an identification of the user resulting from the first authentication method. The second web site 16 would then accomplish the second authentication method to complete authentication of the user. The second web site 16 would then transmit back to the first web site 14 the results of the second authentication, so that the first web site 14 could then accept or deny access to the user.

Ying describes a system for selecting, distributing, and selling fonts. Ying states at col. 23, lines 23-37:

This page includes a field 632 for entering a user name, a field 634 for entering a password, a submit button 636, a link 638 to allow a new user registration; and the links 248 to the store's major pages. If the user presses the submit button 636, steps 642 and 644 will upload a request for log-in processing.

As shown in FIG. 33, when the font store server receives a request for log-in processing, step 648 verifies that the user name and password pair specified in the request are recorded in association with a user ID stored in the server's customer database. If so, step 650 downloads a checkout page for the matching user ID which specified any fonts currently selected for purchase by either the request or the shopping cart stored on the server for the user ID.

Krueger describes a secure networked transaction system. As noted in ¶¶ 9 & 40-44 and Fig. 2-7, Krueger describes a method and apparatus where an end user's card information is verified at a central security server located in a web site different from a merchant's web site.

The Examiner stated that Ying describes "providing a first user authentication method (col. 23, lines 23-37) and a second authentication method (col. 23, lines 43-46), wherein the first and second user authentication methods are selected to authenticate at least one factor associated with the user/password and credit card information (col. 23, lines 23-37)." The Examiner also stated that Ying describes a "credit card processor" being involved in user authentication. The Examiner goes on to say that Ying does not disclose use of [two] web sites. The Examiner stated that Krueger, however, discloses authenticating at both "a first wet site/merchant web page" (¶¶ 40-41) and "[a second] authentication web site/verification system" (¶¶ 43-44).

Appellant has carefully reviewed Ying, and in particular the section cited by the Examiner, to find a "two-factor user authentication" method where two web sites (or servers) are involved in two different authentication methods using at least two factors associated with the user as described by Appellant and claimed in claims 4, 5, 7-9 and 18. Ying does not, however, describe such a two-factor user authentication method occurring at two different web sites (or servers).

It is well known in the security field that authentication can be based on three factors: what you know, what you have and what you are. An authentication based on one of these factors is termed "single-factor authentication." An authentication based on two of these factors is termed "two-factor authentication." Appellant teaches adding a token to a password authenticated web site in order to authenticate not only on what you know (i.e., a password) but also on what you have (i.e., the token). To accomplish this strong level of authentication, Appellant teaches adding a second authentication server and using the second authentication server to authenticate the token-bearing user.

Instead of providing the strong two-factor authentication described and claimed by Appellant, Ying describes a method and apparatus where an end user authentication occurs at a first server (col. 23; Fig. 1, 'Font e-Commerce Server') using a username and a password, and verification of the end user's card information occurs at a second server (col. 23, line 52-64; Fig. 1, 'Credit Card Processor'). Specifically, Ying states at col. 23, lines 43-46:

Step 656 displays the checkout page, including a field 658 for entering a user's credit card number; a field 660 for entering a user's credit card expiration date; a purchase button 662; and the links 248 to the font store's major pages.

Ying also states at col. 23, lines 52-55:

As shown in FIG. 35[,], when the font store server receives a request for checkout processing, step 670 causes steps 672 through 678 [to] be executed. Step 672 sends the credit card number and expiration data specified in the request to a credit card processor 170 of the type shown in FIG. 1.

Ying further states at col. 23, line 65 – col. 24, line 6:

FIG. 36 illustrates that when the browser receives a font download page, step 680 causes steps 682 through 692 to be performed. Step 682 displays the font download page, which includes text 684 explaining how to download the purchase fonts, link 686 for the download of each of the one or more purchased fonts, and the links 248 to the font store's major pages. If a user selects a given purchased-font's download link, steps 690 and 692 will upload a request for the download of the given font's font file.

These disclosures including the portions cited by the Examiner do not, however, describe authentication of the end user at a second site (or server). As noted at col. 23, lines 60-61, Ying describes approving (or verifying) the end user's credit card information without authenticating his identity at the second server. Ying only states a checkout process at col. 23, lines 56-62:

If the charge can go through, the transaction processing system 170 will charge the credit card holder's account 176 and credit the font store's merchant account 186 and indicate that the charge went through to the server. If such credit card approval is obtained, steps 674 and 676 will generate and download a font download page.

Credit card number verification does not test what you know, what you have or what you are. It is not, therefore, user authentication. There is only, therefore, single-factor authentication in Ying.

In contrast to Ying, Appellant teaches and claims that both web sites are involved in user authentication. As noted at p. 3, lines 20-22, Appellant teaches:

The first web site authenticates the user using one authentication method, for example, the username and password. The second web site authenticates the user using the second authentication method.

Ying, therefore, does not describe a user authentication method and system where “both web sites are involved in user authentication using the authentication data” as taught by Appellant and claimed in claims 4, 5, 7-9 and 18.

Furthermore, Ying does not describe an authentication method using at least two factors at two servers. Instead, Ying describes using only single factor authentication (i.e., a password) at one server. As discussed above, ‘Credit Card Processor’ under Ying’s approach uses information related to his credit card. Like a username or password, however, the end user’s card information is at most ‘what the end user knows’ (first factor). The end user’s card information is not ‘what the end user has’ (second factor) such as a token-generated synchronous code enabling the card information processing server to authenticate the identity of the end user. Ying, therefore, does not describe “providing a first and a second user authentication methods selected to authenticate at least two factors associated with the user” as taught by Appellant and claimed in claims 4, 5, 7-9 and 18.

Accordingly, although a username or password and his credit card information are received through ‘Font e-Commerce Server’ and transferred to ‘Credit Card Processor’ under Ying’s approach, they are, at most, one factor of the same type as discussed above. Ying, therefore, does not describes “enabling a user to communicate authentication data for both authentication methods to a first web site” and “enabling the communication of at least some of the authentication data from the first web site to a second web site” as taught by Appellant and claimed in claims 4, 5, 7-9 and 18.

Finally, as noted above, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. The Examiner stated that “it would have been obvious, to one of ordinary skill in the art at the time of the invention, to modify Ying to make use of Krueger’s system, and as such [to] include credit card information to be sent from Ying’s font web site to Krueger’s verification system web site, as part of checkout process, where the user is further authenticated to the verification system web site/verification system web site.” The Examiner goes on to state that “one of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of increased security of the user’s

confidential information.” As support of this, the Examiner points to ¶¶ 9, 40, 41 and 43-44 of Krueger, which state:

[0009] What is desired therefore is a system for allowing a customer to purchase items where the customer is not required to give the PIN number of the debit card to a merchant during an on-line purchase. It is another object of the present invention that the merchant or any party intercepting a communication between the customer and merchant, never has access to the customer’s PIN number throughout the transaction. It is further object of the present invention that all the information required to complete a transaction never exists in one transmission on the public network.

[0040] 1. The customer goes to merchant’s web page and decides to buy something. On the https:// page where they would normally enter a credit card, there is also an option for a Debit/Check card. The customer enters their card number, and clicks the purchase button (buy it, whatever, just like they do now).

[0041] 2. Because it is a Debit Card purchase, the merchant establishes a communications channel with the verification system and sends the card number, merchant ID, and the transaction amount.

[0043] 4. The merchant redirects the customer’s web browser to the verification system server, passing the transaction ID as part of the address.

[0044] 5. The verification system looks up the transaction information corresponding to the transaction ID, and present a page to the customer requesting the information to complete the transaction, such as the PIN number and optionally the symbol, representing the ATM backbone processing network, and/or other information from the card.

Appellant respectfully submits that the above passages simply state another single-factor authentication of the same type (i.e., ‘what a user knows’ such as PIN and credit card information) used to authenticate the user at the merchant site of Ying.

For these reasons as discussed above, Appellant respectfully requests that the Examiner’s rejection of claims 4, 5, 9 and 18 be reversed.

Regarding claim 7, in addition, neither Ying nor Krueger teach or suggest the first web site communicating with the second wet site only if the user is initially authenticated as taught by Appellant and claimed in claim 7.

Regarding claim 8, in addition, neither Ying nor Krueger teach or suggest the first web site communicating to the second wet site at least data relating to the second authentication method as taught by Appellant and claimed in claim 8.

The Examiner rejected claims 21 and 28 as being unpatentable. Claim 21 and 28 require authenticating the user to a first web site of the one or more web sites and authenticating the user

to a second web site as well once authenticated to the first web site. As discussed above, neither Ying nor Krueger, alone or in combination, teach or suggest a method or system that authenticates a user not only in the first site but also in the second site. Under both Ying and Krueger, one site performs verification of the user's information without authenticating his identity as taught by Appellant and claimed in claims 21 and 28.

Nevertheless, the Examiner goes on to state that "one of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of increased security of the user's confidential information." As support of this, in addition to ¶¶ 9, 40, 41 and 43-44 as discussed above, the Examiner points to ¶¶ 61-63 of Krueger.

Appellant, however, respectfully submits that there is no suggestion or motivation to combine a reference that verifies a user's card information at a second server (Ying) with a reference that employs a card verification method over two web sites (Krueger) to form a method and system that authenticates a user not only in the first site but also in the second site as described by Appellant and claimed in claims 21 and 28. Appellant respectfully requests that the Examiner's rejection of claims 21 and 28 be reversed.

Claims 10-12, 19-20, 22-27 and 29-34 were rejected under 35 USC § 103(a)

Claims 10-12, 19-20, 22-27 and 29-34 are rejected under 35 USC § 103(a) as being unpatentable over Ying and Krueger, as applied to claims 21 and 28 above, in further view of "RSA Web-Security Portfolio; How RSA SecureID Agents Can Secure Your Website" (hereinafter 'RSA').

Regarding claims 10-12 [and 19-20], the Examiner stated that "Ying lacks authenticating to the second web site with a token." The Examiner also stated that "RSA teaches that two-factor authentication (p. 2, ¶ 1), which comprises entering a user ID, PIN and a randomly generated authentication code generated by a token (p. 2, ¶ 4), ensures greater security than traditional static password (p. 2, ¶ 1)."

The Examiner goes on to state that "one of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of increased security of the user's confidential information." As support of this, the Examiner points to p. 2, ¶¶ 1-4 of RSA, part of which states:

[¶ 4, lines 2-7]...the user is prompted for a valid user ID, Personal Identification Number (PIN) and a unique, randomly generated authentication code from the RSA SecureID authentication device. These credentials are passed via an SSL connection to the RSA ACE/Server where the PASSCODE is validated.

Ying and Krueger are discussed above. Neither reference discloses adding either user authentication at a second web site or a second factor of authentication to an existing single-factor authentication system.

RSA also fails to show a two-factor authentication method where both web sites are involved in user authentication using at least one authentication data of a different factor and where access to content on the first web site is restricted if the user is not authenticated to both web sites as described by Appellant and claimed in claims 10-13, 16 and 17. As noted above, RSA transfers all the authentication data to the second web site and authenticates a user at a second web site using the PASSCODE.

Appellant, therefore, respectfully submits that there is no suggestion or motivation to combine RSA with Ying and Krueger to form a user authentication system with two different authentication methods each running at a different web site and each using at least one different type of factor, wherein information regarding the second factor is transferred to the second web site only when the user is properly authenticated in the first web site using the first factor as described by Appellant and claimed in claims 10-13, 16 and 17. Appellant respectfully requests that the Examiner's rejection of claims 10-13, 16 and 17 be reversed.

Regarding claims 22, 23, 29 and 30, the Examiner rejected claims 22, 23, 29 and 30 based on analysis of claims 21 and 28. The Examiner stated that, despite the lack of Ying's authenticating to the second web site with a token, this limitation is described by RSA as noted above. The Examiner goes on to state that it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ying, as modified above, such that the user enters at least a randomly generated authentication code to Krueger's verification server, and hence authenticates to the second web site using a token. As support of this, the Examiner pointed to p. 2, ¶ 1 of RSA, which partly states:

Two factor authentication ensures greater Internet security than traditional static password that are easily guessed or compromised, by combining something the user knows (secret PIN) and something the user has (random token code that changes every 60 seconds).

The section cited does not, however, offer a suggestion or motivation for combining one authentication method using a password at a first web site (Ying and Krueger) with another authentication method using a token (RSA) or one-time password at a second web site to form what is described by Appellant and claimed in claims 22, 23, 29 and 30. Appellant teaches and claims an authentication method and system which initially authenticates the user to a first web site and then authenticates the user to a second web site as well once the first authentication is properly performed. Under Appellant's approach, a user is granted access to content on the one or more web sites only if authenticated to both the first and the second authentication web sites. Such an approach is advantageous since it allows the merchant to add strong authentication to existing sites without redesigning the site.

For the reasons discussed above, Appellant respectfully requests that the Examiner's rejection of claims 22, 23, 29 and 30 be reversed.

8. SUMMARY

For the reasons presented above, Appellant respectfully submits that the claims were not properly rejected under 35 U.S.C. §103 since no *prima facie* case of obviousness under 35 U.S.C. §103 has been established. Therefore, it is respectfully requested that the rejections of claims 4, 5, 7-13, 16-23 and 28-30 be reconsidered and withdrawn. An appellant respectfully submits that all of the pending claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone the Appellants' attorney, Thomas Brennan at (612) 373-6909 to facilitate prosecution of this Application. If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

SEAN BRENNAN

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.

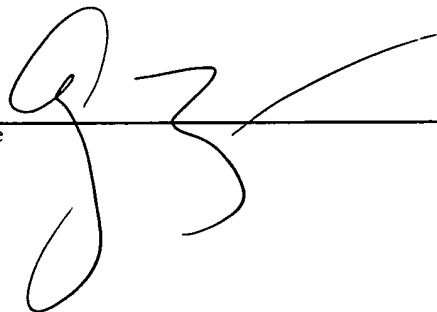
P.O. Box 2938

Minneapolis, MN 55402

Date October 16, 2006 by 
Thomas F. Brennan
Reg. No. 35,075

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Appeal Brief, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 16th day of October 2006.

Amy Moriarty
Name


Signature

CLAIMS APPENDIX

1. (Withdrawn) A method of implementing token-based electronic security across multiple secure web sites, in which the user has a security token, comprising:
 - storing unique token identification information, and the seed value of each token, in a security system;
 - requiring the user, upon login to a secure web site, to enter at least the code generated by the user's token;
 - passing the user's token code from the web site to the security system;
 - using the security system to verify whether or not the user's token code was generated by the user's token; and
 - passing the verification information from the security system to the web site, for use in web site security.
2. (Withdrawn) The method of claim 1 wherein the requiring step further requires the user to enter a user name and user password.
3. (Withdrawn) The method of claim 2 further comprising the step of:
 - the web site verifying the user name and user password before passing the user's token code to the security system.
4. (Rejected) A method of accomplishing two-factor user authentication, comprising:
 - providing first and second user authentication methods, wherein the first and second user authentication methods are selected to authenticate at least two factors associated with the user;
 - enabling a user to communicate authentication data for both authentication methods to a first web site using the internet;
 - authenticating the user at the first web site using the first authentication method;
 - enabling the communication of at least some of the authentication data from the first web site to a second web site using the internet;

authenticating the user at the second web site based on the authentication data transferred from the first web site using the second authentication method; and

wherein both web sites are involved in user authentication using the authentication data and wherein access to content on the first web site is restricted if the user is not authenticated to both web sites.

5. (Rejected) The method of claim 4, wherein the first web site initially authenticates the user based on the data relating to the first authentication method.
7. (Rejected) The method of claim 5, wherein the first web site communicates with the second web site only if the user is initially authenticated.
8. (Rejected) The method of claim 7, wherein the first web site communicates to the second web site at least data relating to the second authentication method, and user-identification data.
9. (Rejected) The method of claim 4, wherein one authentication method employs a password.
10. (Rejected) The method of claim 4, wherein one authentication method employs a token.
11. (Rejected) The method of claim 10, wherein the token is hardware-based, and generates a code that comprises at least some of the data for the authentication method.
12. (Rejected) The method of claim 11, wherein the token is a stand-alone, portable device.
13. (Rejected) The method of claim 11, wherein the token is USB-based and is accessed by a browser.
14. (Withdrawn) The method of claim 10, wherein the token is software-based, and generates a code that comprises at least some of the data for the authentication method.

15. (Withdrawn) The method of claim 14, wherein the token comprises a browser plug-in.
16. (Rejected) The method of claim 4, wherein one authentication method employs a fixed complex code.
17. (Rejected) The method of claim 16, wherein the fixed complex code comprises a public key infrastructure.
18. (Rejected) The method of claim 4, wherein one authentication method is software-based.
19. (Rejected) The method of claim 4, wherein at least one user authentication method can be used across multiple web sites.
20. (Rejected) The method of claim 10, wherein the token is embedded in a cell phone.
21. (Rejected) A method of authenticating a user to one or more web sites, comprising:
authenticating the user to a first web site of the one or more web sites; and
once authenticated to the first web site, authenticating the user to a second web site;
wherein the user is granted access to content on the first web site only if authenticated to both the first and second web sites.
22. (Rejected) The method of claim 21, wherein authenticating to the first web site is performed with a password and authentication to the second web site is performed with a token.
23. (Rejected) The method of claim 21, wherein authenticating to the first web site is performed with a password and authentication to the second web site is performed with a one-time password.
28. (Rejected) An authentication system, comprising:

one or more web sites implementing a first authentication method;
an authentication web site connected to the one or more web sites for implementing a second authentication method;
wherein authentication information for the second authentication method is entered via a first web site of the one or more web sites and transferred from the first web site to the authentication web site; and
wherein a user is granted access to content on the one or more web sites only if authenticated to both the first web site and the authentication web site.

29. (Rejected) The system of claim 28, wherein the first authentication method is based on a password and the second authentication method is based on a token.

30. (Rejected) The system of claim 28, wherein the first authentication method is based on a password and the second authentication method is based on a one-time password.

APPEAL BRIEF UNDER 37 CFR § 41.37

Serial No.: 10/050,752

Docket: 105.215US1

EXHIBIT APPENDIX

None.

APPEAL BRIEF UNDER 37 CFR § 41.37

Serial No.: 10/050,752

Docket: 105.215US1

RELATED PROCEEDINGS APPENDIX

None.